inv. a1

~~CONDITIONAL ACCESS SYSTEM DECODER AND METHOD OF LOADING USER ENTITLEMENTS INTO SUCH A DECODER~~

inv. a2

The present invention relates to a conditional access system decoder and, more particularly, to a method of loading entitlements which a user can acquire so as to access a distributed service within a conditional access system.

A conditional access system allows a service provider to supply its services solely to users having acquired entitlements with regard to these services. Such is the case, for example, in pay-per-view television systems.

As is known to the person skilled in the art, the service supplied by a service provider consists of an item of information scrambled by control words. To descramble the item, the service provider supplies each user with the control words which served for scrambling the item. To keep the control words secret, they are supplied after having been enciphered with an algorithm with key K. The various enciphered control words are sent to the various users in control messages commonly denoted ECM (the abbreviation ECM standing for "Entitlement Control Message"). The control words are deciphered in a secure processor contained in a security element such as, for example, a smart card.

The scrambled item can be descrambled, and therefore read by a user, only with regard to the entitlements allocated to this user. Each user's entitlements are sent in entitlement management messages commonly denoted EMM (the abbreviation EMM arising from "Entitlement Management Message"). The secure processor makes it possible to validate and to record the entitlements which the user has with regard to the service delivered.

According to a known exemplary embodiment of a conditional access system, the service provider supplies each user with a smart card and a decoder. The selecting of the EMM messages is performed by

installing an appropriate configuration of filters contained in the decoder. This configuration is installed on the basis of the reading, by circuits of the decoder, of data contained in the smart card. For this purpose, the user is required to introduce the smart card into the decoder.

When the EMM messages which correspond to the smart card are present in the signal received by the decoder, they are selected with the aid of the filters and transferred to the smart card where the corresponding entitlements are updated and stored.

The EMM messages are issued, in an asynchronous manner, before the issuing of the scrambled service to which they correspond. The user entitlements are thus, for example, very often issued at the least busy times of the night. Furthermore, the user entitlements are required to be frequently renewed without the user being aware thereof.

It follows that a user who wishes to be able to make regular use of the services of a provider is practically compelled to leave the smart card, which the provider supplied him with, permanently in the decoder so that the transferring of the EMM messages from the decoder to the smart card can be performed at the earliest opportunity.

A user who is a subscriber to several service providers possesses as many smart cards as he has subscriptions. In the case where the various service providers share the same decoder, it is possible to envisage the provision of several different smart card readers on the same decoder but in this case, this appreciably increases the price of the decoder. In the more probable case in which the user possesses more smart cards than card readers available on his decoder, it is then almost impossible, for the user, to correctly manage his pool of smart cards so as to acquire at the earliest opportunity all the entitlements to which he may have a right.

The invention aims to solve the aforesaid problems.

To this end it relates to a conditional access system decoder comprising:

- at least one device intended to read and/or to write data from/to a detachable security element supplied by a service provider;

- filters intended to select at least one message for managing entitlements which a user possesses with regard to a service supplied by the provider from among a data stream received; and

- an access control module which is capable of receiving an identification parameter contained in a security element inserted into the decoder; installing a filter configuration as a function of the identification parameter received in such a way as to select an entitlement management message intended for this inserted security element; and transmitting said message to said inserted security element.

According to the invention, the decoder furthermore comprises a module for storing entitlements which is capable of storing the configuration of filters which is installed by the abovementioned access control module; reinstalling, following the erasure of the configuration of filters consequent upon the removal of the security element, the stored configuration of filters which is appropriate to said security element, in such a way as to select entitlement management message intended for said security element when the latter is removed; and storing said message in a memory of the decoder.

According to another aspect of the invention, the module for storing entitlements of the decoder is furthermore capable of detecting the insertion of a security element into the decoder; verifying whether an entitlement management message intended for said inserted security element is stored in the memory of the decoder; and should verification be positive,

transferring said stored message to said inserted security element.

According to a preferred embodiment of the invention, the module for storing entitlements detects the insertion of a security element into the decoder by recording any new installing of configuration of filters by the access control module.

The invention also relates to a method of processing a message for managing entitlements which a user possesses with regard to a service, said method comprising the steps consisting in:

- inserting a detachable security element into a decoder;
- recovering from said security element an identification parameter;
- installing a configuration of filter of the decoder as a function of said identification parameter in such a way as to select an entitlement management message intended for said inserted security element;
- transmitting said message to said inserted security element.

According to the invention, the step of installing the configuration of filter which is appropriate to said security element is followed by a step of storing said configuration and, when said security element is removed from the decoder, causing the erasure of said configuration of filters, the configuration of filters which is appropriate to the removed security element is reinstalled on the basis of the configuration stored during the storage step in such a way as to select an entitlement management message intended for said removed security element.

According to a preferred aspect of the invention, the method comprises an additional step consisting in storing in a memory of the decoder the entitlement management message intended for the removed security element when such a message is selected.

According to another aspect of the invention, the method furthermore comprises the steps consisting in:

- reinserting said security element into the decoder;
- verifying whether an entitlement management message intended for said inserted security element is stored in the memory of the decoder; and
- should verification be positive, transferring said stored message to said inserted security element.

An advantage of the invention is that it allows the acquisition of user entitlements without the security element, which contains the data for installing the configuration of filters allowing the acquisition of these entitlements, being present in the decoder at the moment of acquisition.

Other characteristics and advantages of the invention will become apparent from reading a particular, non-limiting, embodiment of the invention given with reference to Figures 1 to 4, among which:

- Figure 1 represents a decoder furnished with a security element according to the invention;
- Figure 2 diagrammatically represents a data packet transporting a user entitlement management message;
- Figure 3 diagrammatically represents the various events and the various transfers of data involved during the method of processing the user entitlement management messages according to the invention;
- Figures 4a to 4e illustrate various steps of the method according to the invention.

In all the figures, the same references denote the same elements.

Figure 1 represents a conditional access system decoder allowing a user with whom it is set up to receive services, such as televised programs, in the form of a digital information stream coded for example according to the MPEG2 standard (ISO/IEC 13818-1).

Only the elements required for the understanding of the invention have been represented in Figure 1.

The decoder comprises in a manner known per se a tuner/demodulator 17 which receives a signal S, emanating from a satellite antenna or from a cable network, and which outputs a digital data stream, transmitted in the form of packets, and referred to as the TS (standing for "Transport Stream") in the aforesaid MPEG 2 standard, and containing the services supplied by providers.

The services being transmitted in scrambled form, each service provider also supplies the user with a smart card 10 which contains secret elements making it possible to descramble the services.

This smart card 10 is intended to be inserted into a smart card reader of the decoder, only the interface 12 with a microcontroller 16 in which the various applications of the decoder are executed having been represented.

The decoder also comprises a memory 14 which the microcontroller 16 can access in read or write mode.

Finally, the decoder comprises a component 20 referred to as a demultiplexer which receives the data stream TS so as to extract therefrom the video or audio data packets corresponding to a service which the user wishes to display or so as to extract therefrom data packets containing so-called "service" information, such as user entitlement management messages EMM.

The demultiplexer 20 is composed of filters 11 and of a buffer memory 18, generally referred to as a "buffer".

The filters are formed, as is known to the person skilled in the art, of assemblies of comparators receiving on the one hand the data stream TS and on the other hand a reference value making it possible to identify the data packets to be extracted. When data packets are extracted from the stream TS, they are

stored in the buffer 18 before being used by the various applications of the decoder which are executed in the microcontroller 16.

Represented in Figure 2 is a data packet containing a user entitlement management message EMM. Like any data packet transported in the TS stream, it comprises an identifier: the PID (standing for "Packet IDentifier"), followed by so-called "private" data. Indeed, all the data relating to access control are specific to the service provider and are not defined in the transport standard for the data packets.

The private data include the EMM message proper. This message is composed of three elements:

- a first element AD containing the address of the smart card for which the EMM message is intended; it can also entail an address corresponding to a group of smart cards for which the EMM message is intended;

- a second element containing the user's entitlements (subscription, tokens per impulse purchasing of programs, etc); and

- a third element SIGN making it possible to validate the contents of the EMM message which will not be described hereinbelow.

When an EMM message intended for the smart card 10 which is inserted into the decoder has to be extracted from the data stream TS, it is therefore necessary to configure a filter by supplying it with, as reference value, the PID of the data packets transporting the EMM messages and the address of the smart card which is in the decoder.

In what follows, a filter configuration will be said to be "installed" or "set up", meaning that the aforesaid parameters (PID, smart card address) are transmitted to a filter, making it possible to select an EMM message intended for a given smart card.

We shall now describe in greater detail, in conjunction with Figures 3 and 4, the mechanism for recovering the EMM messages intended for a given smart card from the TS stream received.

In Figure 3 we have represented in the form of rectangles the various resources, shared by all the applications of the decoder, which are useful for an understanding of the invention. These shared resources comprise:

- filters 111, which correspond to the filters 11 of Figure 1;

- a smart card reader module 112 which comprises both a hardware part (the circuit for reading/writing on the chip - or integrated circuit - of the card) and a software part making it possible to communicate with the other applications of the decoder;

- a so-called signalling tables recovery module 101 which is a piece of software capable of extracting from the TS stream tables containing information about the structure and the positioning of the data packets in the TS stream. In particular, this module is capable of extracting a table referred to as CAT (standing for "Conditional Access Table") in the aforesaid MPEG 2 standard and which contains, among other things, the PIDs identifying the data packets containing the EMM messages;

- a buffers management module 102 which is a piece of low-level software responsible for allocating and manipulating the buffers used for the storage of the packets which are extracted from the data stream TS by the filters 111.

The various resources just described are used by applications (software) which are represented by circles in Figure 3. Finally, in Figure 3 the data streams are represented by continuous arrows and the events are represented by dashed arrows.

In what follows we shall be interested solely in applications which are useful in the loading of user entitlements within the framework of the invention.

The first application, the CA module is a piece of software specific to a service provider and which implements this provider's conditional access system. Specifically, it is very rare for two different service

providers to use the same conditional access system. In general, the CA module is therefore a piece of secret software, which is known only to the service provider. The manufacturer of the decoder receives it in the form of "object code" (incomprehensible compiled software - as opposed to the "source code" - and which cannot be modified as is) so as to be built into the decoder.

The second application, referred to as the MD entitlements storage module, is, according to the invention, an application module which is independent of the CA module with which it does not communicate directly. The role of this MD module is, as will be seen hereinbelow, to "spy" on the filter configurations installed by the CA module so as to be capable later of receiving EMM messages intended for a smart card which has been extracted from the decoder in place of the CA module.

We shall now describe more precisely the various steps leading to the loading of the user's entitlements onto his smart card.

When the user of the decoder selects a particular service, for example a televised channel, the signalling tables recovery module 101 recovers the CAT table described hereinabove and the CA module recovers from this table (step A1, Fig. 3) the PID identifying the data packets in which the EMM messages for the provider supplying the selected service are transmitted. The PID is then stored by the CA module in the memory 14 of the decoder ("PID STORAGE" step A1a).

If we assume that a smart card No. 1 is inserted into the decoder, then the card reader module 112 generates a "CARD INSERTED" event at step A2. On receipt of this event, the CA module generates a "READ ADDRESS" event in step A3 and obtains, in response from the card reader module 112, the address of the smart card in step A4.

With the aid of this address and of the stored PID, the CA module can install a configuration of filters C1 so as to select the EMM messages intended

for smart card No. 1 (step A5 "SET UP CONFIG.").

Referring now to Figure 4a, represented therein is the assembly 111 of filters F1 to Fn available for the various applications of the decoder. It is assumed that the filter F1 is allocated to another application, it is therefore represented hatched in Figure 4a. The first filter available is filter F2. The latter is allocated to the CA module which therefore installs the configuration C1 into F2.

Returning to Figure 3, it is now assumed that a packet containing an EMM message has been selected by filter F2 which transmits it (step A6) to the buffer management module 102, which generates an "EMM RECEIVED" event for the attention of the CA module (step A7) which responds with a "READ EMM" event (step A8) before receiving the corresponding EMM message (step A9). Finally, the CA module transmits the EMM message to the card reader module 112 (step A10) so that the latter transfers it to smart card No. 1 for processing (updating of the user's entitlements stored in the card). Steps A6 to A10 are repeated as many times as EMM messages intended for smart card No. 1 are received by the filter F2.

Now considering the MD module of the invention, the latter continuously monitors the configurations of filters which are installed by the CA module and, as soon as a new configuration is set up, as in the aforesaid step A5, the MD module recovers this configuration (step B1) and stores it ("CONFIG. STORAGE" step B1a). Figure 4a depicts the end of this last step and it is noted that the configuration C1 installed by the CA module has been stored by the MD module (see "MD STORAGE" array, "CONFIG." column).

Let us now assume that the user removes smart card No. 1. A "CARD REMOVED" event is then generated by the card reader module 112 (step C1). On receipt of this event, the CA module erases the filter configuration C1 corresponding to the removed card (step C2). The filter F2 is therefore freed (Figure 4b).

The MD module which monitors the filters 111 then receives a "CONFIGURATION ERASED" event (step D1) and immediately reinstalls (step D2) the said configuration C1 which had been stored in the previous step B1a. Thus, represented in Figure 4b is the state of the filters at the conclusion of this step D2: filter F1 is still allocated to another application of the decoder; filter F2 has been freed by the CA module and filter Fi has been allocated to the MD module so as to install the configuration C1.

It will be noted in what follows that when a filter is allocated to the CA module, it is represented in Figures 4a to 4e by a continuous bold rectangle, whereas when a filter is allocated to the MD module it is represented by a dashed bold rectangle.

By virtue of the MD module of the invention, the EMM messages intended for smart card No. 1 can therefore still be selected from the data stream TS by filter Fi despite the absence of the said card from the decoder. When such an EMM message intended for card No. 1 is selected, it is transmitted to the MD module (step D3) so as to be stored in a memory of the decoder ("EMM STORAGE" step D3a). Advantageously, the EMM messages are stored in a temporary buffer memory area of the memory 14 of the decoder.

Referring to Figure 4c, it is assumed that a smart card No. 2 is inserted into the decoder. The filter F2 is therefore allocated to the CA module so as to install a configuration C2 making it possible to select EMM messages intended for card No. 2. This configuration C2 is immediately stored by the MD module (see "MD STORAGE" array, "CONFIG." column). In parallel, the filter Fi remains allocated to the MD module with the configuration C1 so as to recover the EMM messages intended for smart card No. 1 which has been extracted. It is assumed that at the end of this step, a message EMM1 intended for card No. 1 has been stored by the MD module (see "EMM" column of the "MD STORAGE" array).

In Figure 4d it is assumed that the card No. 2 has been extracted, filter F2 is therefore again freed and filter F1 which was free has been allocated to the MD module so as to install the configuration C2 stored previously. As far as filter Fi is concerned, it still remains allocated to the MD module with the configuration C1.

Let us now assume that the user reinserts his smart card No. 1 into the decoder. Steps A2 to A5 described previously are then executed and a filter, for example the filter F2 (Figure 4e), is allocated to the CA module with the configuration C1. The MD module, which continuously monitors the filter configurations installed by the CA module, receives this configuration C1 (step E1) and compares it with those already stored (C1, C2). As this configuration C1 is already stored, the MD module then verifies whether EMM messages intended for the corresponding smart card No. 1 are stored and it finds the message EMM1.

The message EMM1 is then transmitted to the ~~pilot~~ buffer management module 102 (step E2) as if it had reached filters 111 directly (as during step A6). Steps A7 to A10 are then replayed and everything happens, from the point of view of the CA module, as if the message EMM1 received had just been selected by filter F2 from the data stream TS.

Thus, by virtue of the invention, the updating of the user's entitlements for card No. 1 is done even if the new entitlements have been received while the card was not inserted in the decoder. Furthermore, an important advantage of the MD module of the invention is that it intervenes in the various resources of the decoder without ever interacting directly with the CA module. The software of the CA module therefore does not need to be modified with respect to the prior art decoders.

When the message EMM1 is transmitted to the ~~pilot~~ buffer management module 102 by the MD module, the latter simultaneously frees the memory space reserved for

storing the message EMM1 (see "EMM" column of the "MD STORAGE" array, Fig. 4e). Figure 4e furthermore depicts the filter F1 which is allocated to the MD module with the configuration C2 and it is assumed that a message EMM2 intended for smart card No. 2 has been received and stored (see "EMM" column of the aforesaid array).

As far as the strategy for freeing the filters is concerned, this depends on the implementation chosen by the developer of the decoder. For example, it is possible as in Figure 4e to choose to free the filter Fi (which was previously allocated to the MD module with the configuration C1) as soon as another filter (here F2) is allocated with the same configuration as Fi.

The description of the preferred embodiment of the invention has been given using the example of the MPEG 2 digital data packet transport standard but the invention naturally applies within the framework of any other data transport standard.